[From the Winter/Spring 2015 Edition of the *White Collar Crime Committee Newsletter,* published by the American Bar Association Criminal Justice Section's White Collar Crime Committee]

Bankers Beware of So-Called "Hotwatch" Orders – Are They Even Legal?

By Craig Denney and Carrie Parker, Snell & Wilmer L.L.P.[1]

The news media regularly publishes reports about sophisticated financial fraud and white collar and corporate criminal schemes that take place on Wall Street and sometimes on main street in the United States. There has been an outcry by elected officials for law enforcement to ferret out financial fraud and money laundering activity in the financial sector.[2] Even a prominent jurist has spoken out on the issue.[3] As a result, this pointed criticism may have spurred federal and state law enforcement to become all the more aggressive in their investigations of targets (including corporations and financial institutions) suspected of aiding and abetting financial fraud and money laundering.

Financial institutions are obligated by federal law and banking regulations to safeguard customer account information. Banks are also obligated to comply with anti-money laundering initiatives to "know their customers." In the past, prosecutors and investigators have routinely relied upon administrative and grand jury subpoenas to obtain business and account records from banks and financial institutions. More recently, however, law enforcement appears to be pushing the envelope in financial investigations.

Rather than utilize traditional tools like subpoenas and seizure warrants, investigators have obtained so-called "Hotwatch" orders to direct financial institutions to monitor in real-time the ongoing and future bank transactions involving customer accounts, including date, time and location of such transactions. In some instances, law enforcement investigators go directly to courts to obtain these orders without having a prosecutor vet them.[4] As such, serious questions exist as to the legal validity of these orders. This article examines these Hotwatch orders and the purported legal authority upon which they are based.

---

[1] Craig Denney and Carrie Parker are litigation attorneys with the law firm Snell & Wilmer L.L.P. Mr. Denney is a former federal prosecutor and Ms. Parker is a former deputy state attorney general. They defend companies and individuals in federal and state grand jury investigations and trials in Nevada and California.

[2] The Hill, Steven Shroeder, "Senators Warren, Shelby: Criminal Bank Execs Should Face Arrest" (Sept. 9, 2014); The Guardian, David Dayen, "Eric Holder Didn't Send a Single Banker to Jail for the Mortgage Crisis: Is That Justice?" (Sept. 25, 2014); http://www.theguardian.com/money/us-money-blog/2014/sep/25/eric-holder-resign-mortgage-abuses-americans

[3] *See* Judge Jed Rakoff's article "The Financial Crisis: Why Have No High-Level Executives Been Prosecuted?" (New York Times Book Review)(Jan 9, 2014 ed.); http://www.nybooks.com/articles/archives/2014/jan/09/financial-crisis-why-no-executive-prosecutions/

[4] In *Freedman v. America Online*, 303 F.Supp.2d 121 (7th Cir. 2005), over-zealous law enforcement officers presented a search warrant application to America Online ("AOL") which had been reviewed or signed by a judge. AOL complied with the invalid warrant, and the person whose email account information had been disclosed sued the law enforcement officers as well as AOL. The claims against AOL were dismissed pursuant to a forum selection clause in the plaintiff's subscription agreement with AOL. The claims against the law enforcement officers survived summary judgment.

If your corporate client or financial institution receives such an order, the first step is to analyze the legal authority purportedly supporting it. The next step is to decide whether to challenge the order or comply with it.

Purported Legal Authority

The authors are aware of Hotwatch orders purporting to rely upon federal statutes related to wiretaps, pen registers and trap and trace devices, and the All Writs Act. We will briefly review each of these statutes below. None of them, however, provide valid authority for such expansive law enforcement orders.

Wiretaps and Stored Communications

Title III electronic surveillance orders (also known commonly as wiretaps) require probable cause and have a detailed application process with strict limitations.[5] These powerful orders authorize law enforcement to listen and monitor telephone and electronic communications in real time. Due to their invasive nature, they require detailed scrutiny and approval by a U.S. District Court to authorize them. Federal law enforcement must submit applications to the Justice Department's Office of Enforcement Operations ("OEO") for review and approval before a prosecutor can submit them to a federal judge for approval.[6] A senior DOJ official must also provide a memorandum that is included with the prosecutor's application. Wiretaps are utilized by law enforcement only after exhaustion of traditional investigative tools (*e.g.*, search warrants, subpoenas, grand jury, informants). Title III does not authorize Hotwatch orders.

Reliance upon the Stored Wire and Electronic Communications and Transactional Records Access Act, 18 U.S.C. § 2701 et seq., ("SCA"), to authorize real time tracking of financial transactions associated with a particular bank or credit card account is also suspect. The SCA applies to electronic communication service[7] providers and providers of remote computing services[8] in relation to information about wire or electronic communications.[9] Banks and financial institutions are not electronic communication service providers or providers of remote

---

[5] *See* 18 U.S.C. § 2510-2522.

[6] *See* http://www.justice.gov/criminal/oeo/

[7] The definitions section defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

[8] "Remote computing service" is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

[9] For purposes of the SCA, "electronic communication" is defined as follows:

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but <u>does not include</u>—
> (A) any wire or oral communication;
> (B) any communication made through a tone-only paging device;
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
> (D) <u>electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds</u>.

18 U.S.C. § 2510(12) (emphases added).

computing services. Additionally, electronic funds transfer information is specifically excluded from the definition of an "electronic communication."[10] Finally, the SCA, as its name indicates, applies to *stored* records, not future transactions.[11] Thus, it is unclear how a court could determine the SCA applies to a financial institution or credit card company and the financial transaction information typically sought in a Hotwatch order.

Pen Register or Trap and Trace Device

Reliance on the Pen Register and Trap and Trace statutes do not support Hotwatch orders. Such laws permit installation and use of a pen register or trap and trace related to telephone lines and computer network communications.[12] Pen registers and trap and trace orders allow collection of information related to times and numbers of calls made and received.[13] Orders for these devices do not authorize real time monitoring or disclosure of the actual contents of the calls or the location of a person making or receiving calls.[14] Moreover, these tools do not apply to records of financial transactions, which of course are not telephone calls. Additionally, real-time tracking of financial transaction information would reveal locations of transactions, as well as amounts and types of transactions, which could be analogous to the content of a phone call (if this law applied to financial transaction records).[15]

All Writs Act, 28 U.S.C. § 1651

In a federal case involving the government's attempt to track cell-site locations on a real-time basis, the Department of Justice argued that if the SCA did not provide authority for such real-time tracking, then the All Writs Act, 28 U.S.C. § 1651, authorized such tracking.[16] In an attempt to analogize cell-site locations to credit card transactions, the government argued the All Writs Act authorized "'hotwatch' orders that 'direct a credit card issuer to disclose to law enforcement each subsequent credit card transaction effected by a subject of investigation immediately after the issuer records that transaction.'"[17] The All Writs Act authorizes federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and

[10] 18 U.S.C. § 2510(12)(D).
[11] For a more detailed discussion of investigative techniques related to the SCA, see U.S. Department of Justice, *Search and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* at x (2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.
[12] 18 U.S.C. § 3123(b).
[13] The definition of pen register excludes devices or processes used for billing or cost accounting. 18 U.S.C. § 3127(3).
[14] 47 U.S.C. § 102(a)(2); *United States v. Espudo*, 954 F.Supp.2d 1029, 1039 (S.D. Cal. 2013).
[15] Even if the authority for a pen register or trap and trace device were combined with the SCA, courts addressing the issue have concluded that this does not allow collection of real-time or prospective location data unless the government first makes a showing of probable cause (as opposed to just subpoenaing the information as a business record of the cellular provider). *Espudo*, 954 F.Supp.2d at 1038-43
[16] *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information*, 396 F.Supp.2d 294, 325-26 (E.D.N.Y. 2005).
[17] *Id.* at 326 n.24 (quoting the government's Reply at 8-9).

agreeable to the usages and principles of law."[18] No court has directly addressed whether this language authorizes Hotwatch orders for real-time tracking of financial transactions.[19]

Decide whether to challenge the order or comply with it.

Law enforcement officers may apply for Hotwatch orders from the court without first discussing or vetting the applications with a prosecutor. The application may seek "real time" data from the company or bank that will be extremely cumbersome to comply with.[20] Most federal prosecutors require law enforcement agents to present applications to the United States Attorney's Office *before* going to see a magistrate or federal judge. State prosecutors may not have the same luxury of seeing the application and order until *after* it has already gone to the judge.

Contacting the prosecutor directly may be the most expeditious step by defense counsel before having to challenge the Hotwatch order in court. The benefits are apparent: (1) it alerts the prosecutor to what may be the rogue actions of a law enforcement officer and (2) serves as a 'meet and confer' with the prosecutor about the order and the questionable authority behind it before the recipient must decide whether to comply with or challenge the order in court.

Hotwatch orders are relatively new, and the procedural mechanism to challenge them in court is somewhat unclear. If the company or financial institution decides to challenge the order (or administrative subpoena or letter) in court, options may include filing a motion to quash,[21] filing a motion to modify or reconsider the order,[22] and/or initiating a civil action for an injunction or civil damages.[23] The proper procedural mechanism will depend on the specifics of the case, including the purported authority for the Hotwatch order, whether it is an administrative subpoena or an order issued by a court, and any applicable jurisdictional rules and procedures.

---

[18] 28 U.S.C. § 1651(a). Be wary of a state court Hot Watch order relying upon the All Writs Act, which applies only to the United States Supreme Court and courts established by an Act of Congress.

[19] *In re Application of the United States*, 396 F.Supp.2d at 326 n.24 (explaining the same).

[20] While companies and financial institutions desire to comply with the law, they also do not want to discourage business by acting as a "corporate informant" for law enforcement on their customers. *See Ameritech Corp. v. McCann*, 403 F.3d 908 (7th Cir. 2005) (requiring Wisconsin to compensate telecommunications company for Wisconsin law enforcement's use of the SCA to require the company to generate phone records).

[21] *See* F. R. CRIM. P. 16 ("At any time the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief.); 18 U.S.C. §2703(d) ("A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.").

[22] *See State v. Western Union Fin. Servs.*, 220 Ariz. 567, 208 P.3d 218 (Ariz. 2009) (court's supervisory powers and criminal procedure rules); F. R. CIV. P. 60 (relief from order based on mistake, oversight, or omission).

[23] The SCA provides for a private right of action for someone aggrieved by a violation of the SCA. *Citizens Bank of Penn. v. Reimbursement Tech.*, 2014 WL 2738220 (E.D. Penn. 2014) (discussing what constitutes a sufficient basis to sue for violation of the SCA and noting who is an "aggrieved person" under the SCA). For example, a person may sue law enforcement personnel for the violation when his email account information has been turned over to law enforcement who never presented the search warrant to a court for review and signature but presented it to the email provider as if it was a valid search warrant. *Freedman v. Am. Online*, 303 F.Supp.2d 121 (D. Conn. 2004). Suits against the United States may be brought under 18 U.S.C. § 2712 for willful violations of the SCA or Title III. As discussed more fully above, the SCA may not apply to financial institutions. As such, no court has decided whether the civil action provision of the SCA may provide a financial institution with a private right of action against law enforcement for abusing the SCA to provide access to financial records.

If the company or financial institution decides to comply with the order, and it is based on the SCA, the corporation or bank may find comfort that the SCA provides protections in relation immunity from civil liability for good faith compliance,[24] and recovery of costs.[25] Additionally, both the Wiretap statutes and the Pen/Trap statute provide a statutory good-faith defense.[26] These defenses apply not only to law enforcement but also to providers and other private parties who conduct surveillance in good faith reliance on a court order obtained by law enforcement.[27]

The danger with blindly complying with Hotwatch orders is that they have questionable legal authority, and compliance may set a dangerous precedent for more frequent abuse of law enforcement tools to easily obtain private financial information and sensitive data without investigators complying with the law.

---

[24] Section 2703(e) provides that there may be no cause of action against a provider of wire or electronic communication service for providing information etc. in accordance with the terms of a court order, warrant, subpoena, statutory authorization or certification under the SCA.

[25] Section 2706 provides that the "governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as a reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored." *Accord Ameritech Corp. v. McCann*, 403 F.3d 908 (7th Cir. 2005).

[26] 18 U.S.C. § 2520(d) (good-faith defense for Title III violations); 18 U.S.C. § 3124(e) (good-faith defense for Pen-Trap statute violations).

[27] 18 U.S.C. § 2707(e); s*ee Jacobson v. Rose*, 592 F.2d 515, 522-23 (9th Cir. 1978) (holding good faith defense was available to telephone company which allegedly assisted in wiretap under the belief that it was complying with court order).